The Identification Process Deconstructed

NIST Smart Card Workshop

July 8-9, 2003

The Issue

- Is Identification a Policy Problem or a Technology Problem
- The Answer is It's Both
- Challenge is Understanding What is Policy and What is Technology
- To Facilitate that Process We Recommend "Deconstructing the Identification Process"

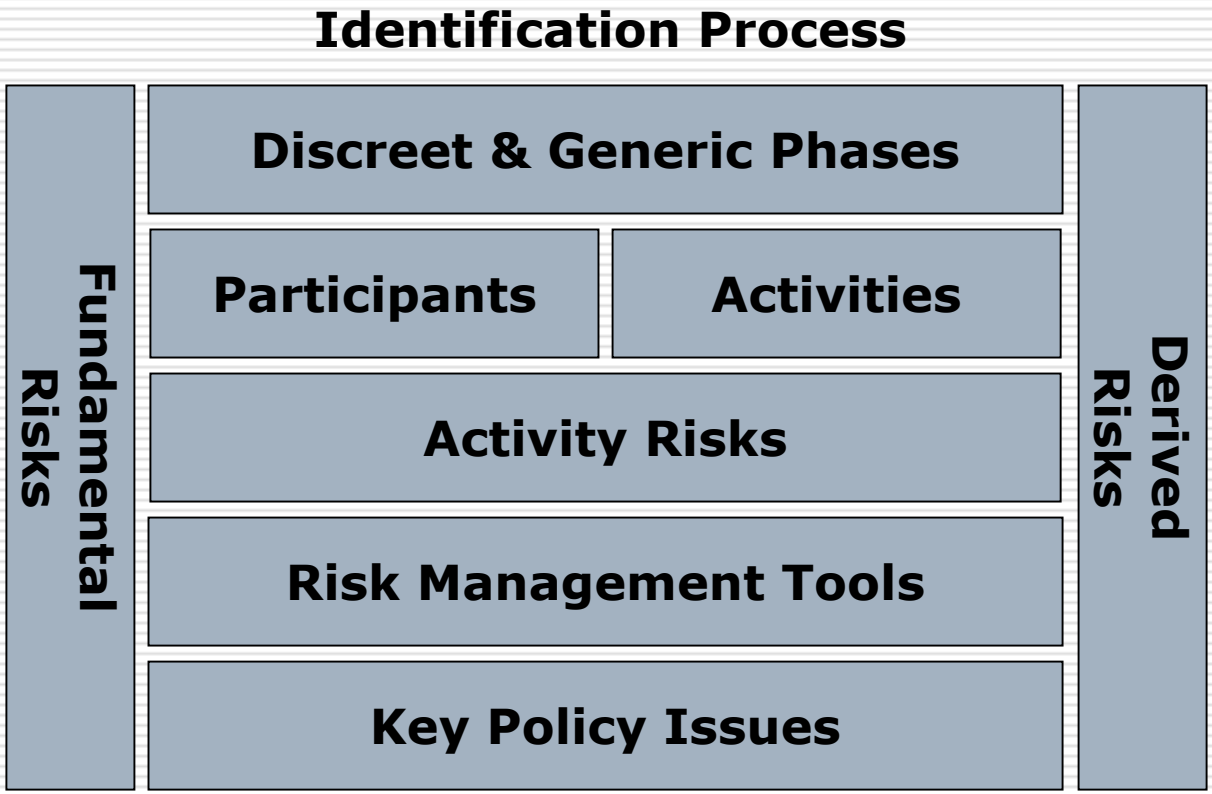
Basic Assumptions

- Identification Process Can be Broken Down into Discreet & Generic Phases
- Three Principal Participants in the Process: Subject, Credentialing Authority, & Relying Party
- Participants Perform Different Activities Based upon Their Roles in Process

Basic Assumptions cont'd

- Identification Process Carries Three Types of Risk: Fundamental Risk, Activity Risk, and Derived Risk
- Finite Set of Risk Management Tools Available to the Participants
- Limited Number of Key Issues Determine Overall Viability of Identification Process or Scheme

Holistic View of the Identification Process



The Principal Participants

- Subject
  - Individual or Object Wishing or Required to be Identified
- Credentialing Authority (CA):
  - Trusted Organization Responsible for Identity Proofing of Subject and Issuing Identity Credential
- Relying Party (RP)
  - Organization Wishing to Identify Individual or Object

Generic Phases of the Identification Process

1. Identity Proofing by Credentialing Authority
2. Creation of Identity Credential
3. Presentation of Identity Credential to Relying Party
4. Acceptance of Credential by Relying Party

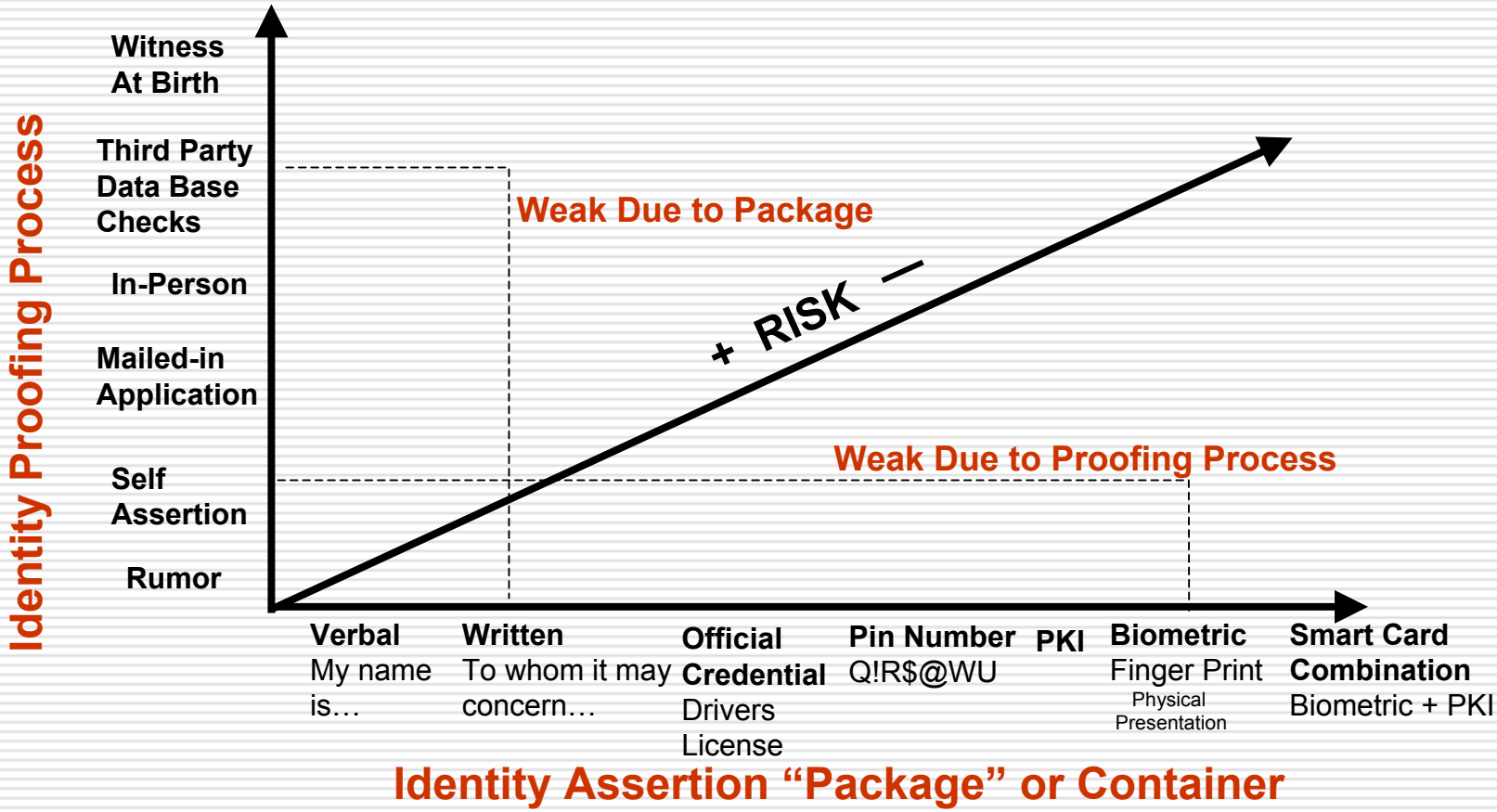
Phase One: Identity Proofing by Credentialing Authority (CA)

- Principal Activities in Phase One
  - Application by Subject
  - Investigation of Subject by CA
  - Identity Assertion about Subject by CA
  - In Closed System CA May also Provision Subject's Domain Rights & Privileges

Phase Two: Creation of Identity Credential

- Principal Activities in Phase Two
  - "Packaging" of Identity Assertion into Identity Credential
    - Key Decision Re: Form Factor of Credential
      - Password, Smart Card, Digital Certificate, etc.
    - N.B. Credential is Symbol of CA's Identity Assertion about Subject; Credential is Not Necessarily Subject's Identity
      - e.g. Flag is Symbol of Freedom; Flag is not Freedom
  - Delivery of Identity Credential to Subject

Identity Assurance is a Function of the Combination of the Strength or Rigor of the Identity Proofing Process and the Strength or Security of the Identity Assertion "Package" or Container



Critical Decisions Facing Credentialing Authority

- Level of Rigor Employed in Identity Proofing Process
- Form Factor for Identity Credential
  - E.g. Password, Digital Certificate, Biometric, Smart Card

Phase Three: Presentation of Identity Credential to Relying Party

- Principal Activities in Phase Three
  - Transportation of Credential to Relying Party
  - Presentation of Credential to Relying Party

Phase Four: Acceptance of Credential by Relying Party

- Principal Activities in Phase Four
  - Prove Subject's Ownership of Identity Credential
    - Primary Function of Biometrics
  - Authenticate Credential (Not Counterfeit)
  - Validate Credential (Current/Use)
  - Acceptance of Credential
  - In Open System RP May Provision Subject's "Domain Specific" Rights & Privileges

Critical Decisions Facing Relying Party

- Whose Identity Credentials will be Accepted & Why
- What Form Factor will be Required

Types of Risk in Identity Process

- Fundamental Risks
  - Risks Associated with Participant's Role in Identification Process
- Activity Risks
  - Risks Associated with Activities Performed by Participants in Identification Process
- Derived Risks
  - Consequential Risks Resulting from Realization of Activity Risk and/or Fundamental Risks

Examples of Fundamental Risks

- Credentialing Authority
  - Misidentify Subject
- Subject
  - Identity Theft
- Relying Party
  - Unauthorized Subject Granted Access

Examples of Activity Risks

- Data Lost, Stolen, or Tampered with During Application, Identity Proofing, and/or Storage
- Data Lost, Stolen, or Tampered with in Transit to Relying Party
- Data Lost, Stolen, or Tampered with During Proof of Ownership, Authentication, and/or Validation Process

Examples of Derived Risks

- Reputation Risk
  - Resulting from Mis-identification (CA) or Unauthorized Access (RP)
- Financial Risk
  - Consequential damages from Mis-identification (CA) or Unauthorized Access (RP)

Outsourcing Activities

- RPs and CAs may elect to outsource the performance of various activities related to their role in the identification process.
- Outsourcing may increase both fundamental risks and activity risks as it may introduce additional management requirements on the participants and technological complexity into the process.
- Outsourcing activities does not create new phases; it sub-divides the four generic phases.

Technology-Based Sources of Activity Risks*

- Data Collection
- Data Communication
- Data Processing
- Data Storage and Retrieval

* In all cases the risk is that data is lost, stolen, or tampered with.

Primary Risk Management Tools

- Policies, Procedures & Controls
- Technology
- Security Assessment
- Audit

Key Issues in Determining Viability Identification Process

- Who Can/Will be Trusted as CA
- Required Degree of Certainty in Identification Process
- RP's Need for Recourse to CA; CA's Willingness to Accept Liability
- Security, Complexity, and Scalability of Implementation
- Process Cost and Ease of Use

Q & A / Contact Information

J. Scott Lowry

Caradas, Inc.

scott@caradas.com

801.554.0430